Intelligent Data Loss Prevention

Get actionable intelligence on the highest risk threats to your sensitive data

Protect your sensitive data from unintentional leaks or malicious breaches. By combining the power of McAfee® Data Loss Prevention (McAfee DLP) with Securonix Threat & Risk Intelligence, organizations get actionable risk intelligence and analytics to protect their sensitive data. The Securonix solution uses techniques based on intelligent behavior and peer group analytics to detect hidden trends and risk-rank data loss prevention (DLP) violations. It builds a prioritized queue of DLP violations, which enables security professionals to focus their investigations on "true" threats and perform in-depth investigations, with extensive visibility into the business and identity context on these alerts.

McAfee Compatible Solution

- Securonix Threat & Risk Intelligence 3.1
- Securonix Application Intelligence 3.1
- Securonix Identity Intelligence 3.1
- McAfee Data Loss Prevention version 9

Today's targeted attacks, whether launched by insiders or by external hackers, have primarily focused on stealing sensitive data stored in structured or unstructured forms. To combat these complex threats effectively, organizations require a comprehensive security intelligence platform that will aggregate, correlate, detect, and risk-rank threats so that security professionals are able to focus their efforts and limited resources on the threats that pose the most significant risk to their data. Securonix and McAfee have joined forces to deliver a security intelligence solution to detect, investigate, and, ultimately, prevent these advanced targeted threats.

Context-Aware Analytics

To identify advanced targeted threats, the Securonix solution brings all DLP violations together for in-depth analysis, aggregating all DLP alerts generated across the McAfee Data Loss Prevention products through an integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, the industry's leading security and compliance management platform. By correlating all DLP violators with the user identity data stored in the organization's HR system, Securonix adds identity context to each alert. This provides security professionals with a single view of all DLP violations performed by the user across the endpoint, email, network, and removable devices/media. Additionally, security professionals can perform advanced analytics on this data cube, including traversing the data from any dimension and performing comparisons across multiple peers for the user.

Threat Identification and Quantification

The Securonix solution analyzes all incoming DLP alerts and quantifies the risk for these alerts. In order to accurately quantify the risk, Securonix uses behavior analysis, peer group analysis, and user-defined threat policies. Using patented behavior profiling techniques, Securonix identifies abnormal patterns in DLP alerts and assigns them a higher risk rating, requiring further investigation. This technique considers more than 120 behavior characteristics spanning time windows, frequencies, network sources, and alert metadata.

By comparing DLP alerts generated for a user with multiple peers for the user, the solution eliminates false positives and accurately quantifies the risk for the alerts that pose the most threat to your data.

Organizations can use the identity and business context in conjunction with the DLP alert data to generate their own set of policies for continuous monitoring and risk quantification. The risk-ranked DLP alerts that are true threats to your data are shown in a prioritized queue for security administrators to act on.

Key Advantages

- Risk-ranked list of DLP alerts for focused investigations
- Enhanced DLP alerts with business and identity context
- Behavior analysis to reduce false positives and pinpoint real and complex data loss situations
- Context-aware policies for continuous monitoring and alerting
- Continuous identification of sensitive data in enterprise applications

Threat Investigation and Management

The Securonix solution provides end-to-end threat investigation and management capabilities. Securonix assigns a unique case ID to each threat that can be assigned to and acted upon by the appropriate owners. The case management capability within Securonix allows for several actions, including re-routing, delegation, and risk acceptance by entering compensating controls and case closure. Each action taken by the case owner is audited for tracking and compliance reporting.

The Securonix solution provides unprecedented visibility to the IT environment for in-depth investigations. By adding business and identity context to DLP alerts, the solution provides tremendous intelligence to security professionals, allowing them to make informed decisions.

Sensitive data Identification and tagging

Sensitive data can include trade secrets, product plans, personally identifiable data, sales quotes, proposals, credit card records, and other information, and these reside in various formats and data stores across the enterprise. It is not uncommon for this data to be in collaborative business applications such as SAP, Siebel, and other business applications.

The Securonix product connects to key business applications and obtains the specific data that has been pre-defined as sensitive by the organization. In SAP applications for example, specific bill of material, master receipt, HR, and vendor information can be found and obtained continuously.

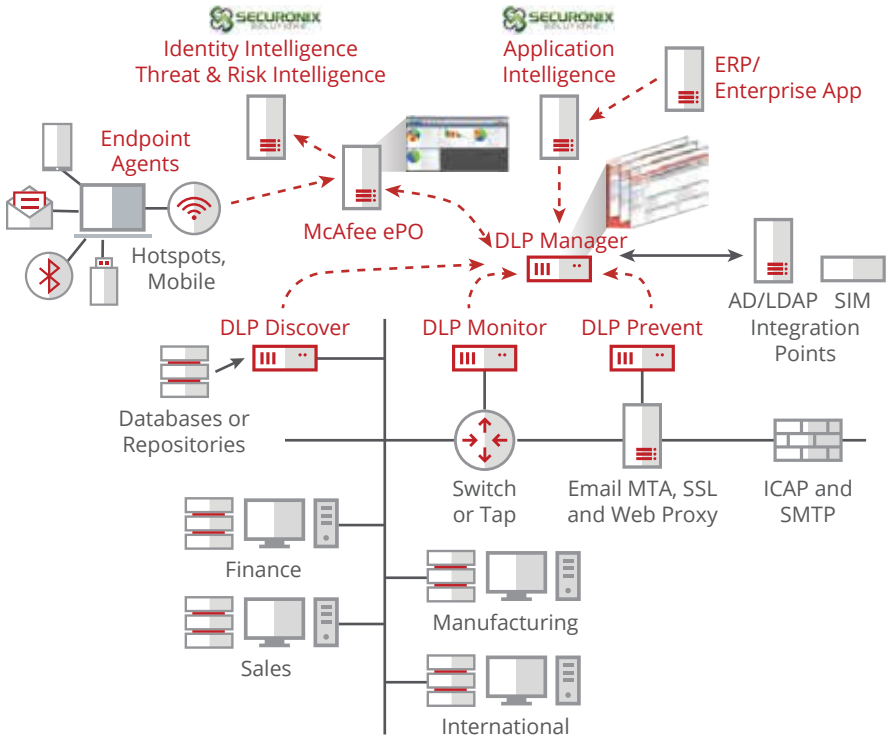

Figure 1. Intelligent DLP deployment architecture.

Securonix integrates with the specific applications to ensure that the intellectual property/confidential information is updated in near real time. Securonix generates data combinations and rules which are then passed to McAfee DLP Discover appliance as fingerprints. When these are complete, Securonix sends the fingerprint data to the McAfee DLP appliance, so that data can be identified when

traversing the network as sent by the end users. The McAfee DLP Endpoint agents are configured to track all access to the application data with the McAfee DLP appliance, restricting potentially damaging transmission attempts.

About Securonix Security Intelligence Platform

Securonix provides the industry's first behavior-based signature-less anomaly detection engine that features advanced identity correlation, automated risk scoring, and abnormality detection for access and activities. For further information, email **sales@securonix.com**.

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management plat-form. With its single agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

Approach

- Fingerprints data automatically for McAfee DLP monitoring
- Gives identity, business, and behavior context to events in the McAfee ePolicy Orchestrator (McAfee ePO) management platform
- Scores DLP events and pushes scores and context back to McAfee ePO software for better management

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

44806brf_securonix_0512
MAY 2012